Introduction to Algebraic Number Theory

BdMO Special Camp 2022

Atonu Roy Chowdhury
atonuroychowdhury@gmail.com

August 23, 2022

In this note, I shall assume that the reader is familiar with basic number theory as well as some intermediate concepts such as orders, primitive root, quadratic residue etc. Last year I prepared a note for those topics, which can be found in https://atonurc.github.io/assets/ord_primroot.pdf. No background in abstract algebra is needed. However, I presume the readers are familiar with the basic definitions of groups.

§1 Rings and Fields

Rings are sets where you can add two elements and multiply two elements. You can think of rings as generalization of $\mathbb{Z}$. In $\mathbb{Z}$ you can add, subtract, multiply two numbers, but not divide. Let's dive into the formal definition of ring.

Definition 1.1 (Ring)**.** A **ring** is a nonempty set R equipped with two binary operations $+$ (addition) and $\cdot$ (multiplication) such that the following properties hold:

(i) $a+b \in R$ for every $a, b \in R$.

(ii) $(a+b)+c = a+(b+c)$ for every $a, b, c \in R$.

(iii) $a+b = b+a$ for every $a, b \in R$.

(iv) There is an element $0 \in R$ (additive identity) such that $0+a = a$ for every $a \in R$.

(v) For every $a \in R$, there exists an element $-a \in R$ such that $a+(-a) = 0$.

(vi) $a \cdot b \in R$ for every $a, b \in R$.

(vii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for every $a, b, c \in R$.

(viii) There is an element $1 \in R$ (multiplicative identity) such that $1 \cdot a = a \cdot 1 = a$ for every $a \in R$.

(ix) Multiplication is distributive over addition, i.e., for every $a, b, c \in R$,

$$(a+b) \cdot c = a \cdot c + b \cdot c \quad \text{and} \quad a \cdot (b+c) = a \cdot b + a \cdot c\,.$$

If a ring does not contain 1, it is called **rng** – ring without ***i***dentity. A ring where multiplication is commutative, i.e. $a \cdot b = b \cdot a$ for every $a, b \in R$, is called a commutative ring. In this note, a

ring is always commutative unless stated otherwise. Also, we shall drop the $\cdot$ and simply write ab instead of $a \cdot b$.

Examples of rings are all over us. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all rings under the usual addition and multiplication. Integers modulo n, $\mathbb{Z}/n\mathbb{Z}$ is also a ring. It's often written as $\mathbb{Z}_n$. The set $\mathbb{Z}[x]$ of all polynomials over integers (polynomials whose coefficients are in $\mathbb{Z}$) is also a ring. In fact, if R is a ring, then the set $R[x]$ of all polynomials over R is a ring, where addition and multiplication are defined in the usual way. A non-example is $\mathbb{N}$ under the usual addition and multiplication. Because the additive inverses of positive integers are not in $\mathbb{N}$[1].

Definition 1.2. An nonzero element $a \in R$ is called a **zero divisor** if there exists another nonzero element $b \in R$ such that $ab = 0$. A ring R is called **integral domain** if it does not contain any zero divisor. In other words, $ab = 0$ implies that at least one of a and b are 0.

If n is not a prime number, then $\mathbb{Z}_n$ is not an integral domain. Because if $n = ab$ for $a, b > 1$, then $ab = 0$ in $\mathbb{Z}_n$ and $a \neq 0$, $b \neq 0$.

Definition 1.3. A nonzero element $a \in R$ is said to be a **unit** if it has a multiplicative inverse. In other words, there exists $b \in R$ such that $ab = 1$. A ring where all nonzero elements are units is called a **field**.

The reason why we require all the nonzero elements to be units instead of all elements is that 0 can never have a multiplicative inverse. Because $0 \cdot a = 0$ for every $a \in R$.

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \implies 0 \cdot a = 0 \,.$$

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all fields. But $\mathbb{Z}$ is not. Neither is $\mathbb{Q}[x]$ or $\mathbb{R}[x]$ or $\mathbb{C}[x]$. One can easily verify that the set of Gaussian integers

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is also not a field. But it has more structres than a ring, which we shall see later.

§2 Applications in Solving Diophantine Equations

First, we shall see an elementary example.

Exercise 2.1
Find all pairs of integers (x, y) such that $x^3 = y^2 - 4$.

Solution. The case y is even is left as an exercise for the reader. In that case, the only solutions are $(0, \pm 2)$. Now we shall solve for odd y. If we factorize the LHS, we obtain

$$x^3 = (y + 2)(y - 2) \,.$$

Since y is even, $\gcd(y + 2, y - 2) = 1$. Therefore, both $y + 2$ and $y - 2$ must be perfect cubes.

$$y + 2 = a^3 \quad \text{and} \quad y - 2 = b^3 \,.$$

[1] I think I should clarify. In this note I shall use the convention that $0 \in \mathbb{N}$.

But then we find that $a^3 - b^3 = 4$. In particular, $a - b \mid 4$. Then

$$\frac{4}{a-b} = a^2 + ab + b^2 = (a-b)^2 + 3ab$$

yields contradiction for each of the possibilities $a - b = 1, 2, 4$. Therefore, there are no solutions when y is odd. ■

Now, what sort of techniques were used in solving this diophantine equation? We used divisibility, primes, gcd etc. From $x^3 = (y+2)(y-2)$, we deduced that both $y+2$ and $y-2$ are perfect cubes given that $\gcd(y+2, y-2) = 1$. What is the reasoning behind this?

If p is a prime factor of x, and $p^\alpha \| x$, then $p^{3\alpha} \| x^3$. Since $y+2$ and $y-2$ are coprimes, p divides only one of those. Thus either $p^{3\alpha} \| y+2$ or $p^{3\alpha} \| y-2$. Notice that we implicitly used fundamental theorem of arithmetic here. That is, every integer has a unique factorization into primes. Now we shall try to use similar ideas in solving another diophantine equation.

Exercise 2.2

Find all pairs of integers (x, y) such that $x^3 = y^2 + 2$.

Firstly, note that y cannot be even. This is seen by taking mod 4 on both sides. Hence, both x and y are odd. Now, can we factorize it like we did it for the previous example? Well, we cannot factorize it in our familiar realm of integers. We have to extend our *umwelt*. That is, we have to involve complex numbers.

$$x^3 = y^2 + 2 = \left(y + \sqrt{2}i\right)\left(y - \sqrt{2}i\right) .$$

Then can we say that $\gcd\left(y + \sqrt{2}i, y - \sqrt{2}i\right) = 1$ (whatever that means)? After that, as argued before, if $p^\alpha \| x$ for a prime p, then either $p^{3\alpha} \| y + \sqrt{2}i$ or $p^{3\alpha} \| y - \sqrt{2}i$. Then we can say that both $y + \sqrt{2}i$ and $y - \sqrt{2}i$ are perfect cubes.

But does any of these make any sense? First of all, what does it mean for the gcd of two complex numbers? Then, what is a prime here? Also, what do we mean by perfect cube in this case? Clearly, the cube of no integer is $y + \sqrt{2}i$ or $y - \sqrt{2}i$. So what do we mean by all these nonsenses?

As we said, we have to extend our familiar realm $\mathbb{Z}$. We shall consider the ring $\mathbb{Z}\left[\sqrt{2}i\right]$, which is the set of all numbers of the form $a + b\sqrt{2}i$ with $a, b \in \mathbb{Z}$.

$$\mathbb{Z}\left[\sqrt{2}i\right] = \left\{a + b\sqrt{2}i \mid a, b \in \mathbb{Z}\right\} .$$

Now we shall see if these complex numbers behave like integers. Firstly, one important feature of integers is that you can perform Euclidean division on them. In other words, given $a, b \in \mathbb{Z}$ with $b \neq 0$, there exist $q, r \in \mathbb{Z}$ such that

$$a = bq + r \text{ and } 0 \leq r < |b| .$$

Can we imitate Euclidean division on $\mathbb{Z}\left[\sqrt{2}i\right]$? The elements of $\mathbb{Z}\left[\sqrt{2}i\right]$ are complex numbers. Even if we can achieve $a = bq + r$, how can we check whether $0 \leq r < |b|$ holds or not? There are no order in $\mathbb{C}$, so it doesn't make any sense to talk about $0 \leq r$. Luckily, we don't have to deal with whole $\mathbb{C}$, so there is a way out. We shall consider the norm function

$$N\left(x + y\sqrt{2}i\right) = x^2 + 2y^2$$

and we imitate Euclidean division as follows: for every $a, b \in \mathbb{Z}\left[\sqrt{2}i\right]$ and nonzero b, there exist $q, r \in \mathbb{Z}\left[\sqrt{2}i\right]$ such that

$$a = bq + r \text{ and } r = 0 \text{ or } N(r) < N(b) .$$

A ring where such a suitable norm function exists is called an **Euclidean Domain**, or ED in short. Now let's see the formal definition.

Definition 2.1 (Euclidean Domain)**.** An integral domain R is called an **Euclidean Domain** if there exists an *Euclidean function* $N : R \setminus \{0\} \to \mathbb{N}$ such that

(i) $N(ab) \geq N(b)$ for all $a, b \neq 0$.

(ii) If $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $N(r) < N(b)$.

According to this definition, $\mathbb{Z}\left[\sqrt{2}i\right]$ is an ED. Verifying that the norm function has the desired properties is left as an exercise.

Another very important property of integers is that of unique factorization into primes. But what even do we mean by primes in $\mathbb{Z}\left[\sqrt{2}i\right]$? Or in general rings?

Definition 2.2 (Irreducible and Primes)**.** We say $a \in R$ is **irreducible** if $a \neq 0$, a is not a unit, and if $a = xy$, then x or y is a unit. We say $p \in R$ is **prime** if p is nonzero, not a unit, and whenever $p \mid xy$, either $p \mid x$ or $p \mid y$.

Our usual definition of primes matches more with irreducibles than primes in a general ring. Don't you worry. Irreducible and prime actually mean the same thing when there is a notion of unique factorization. But we define such a ring in terms of unique factorization into irreducibles.

Definition 2.3 (Unique Factorization Domain)**.** An integral domain R is a **Unique Factorization Domain** (UFD) if

(i) Every non-unit may be written as a product of irreducibles.

(ii) If $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ with p_i, q_j irreducibles, then $n = m$ and we can rearrange them in such a way that $p_i \mid q_i$ and $q_i \mid p_i$.

The condition $p_i \mid q_i$ and $q_i \mid p_i$ can be rephrased as $p_i = u_i q_i$ for some unit u_i. Because

$$p_i = cq_i \text{ and } q_i = dp_i \implies q_i = cdq_i \implies cd = 1 .$$

Now we shall state a couple of theorems without proof.

Theorem 2.1

Suppose R is a UFD. Then $p \in R$ is irreducible if and only if p is a prime.

Theorem 2.2

If R is an ED, then R is a UFD.

Then we shall define gcd of two elements in the old-fashioned way.

Definition 2.4 (Greatest Common Divisor)**.** $\gcd(a,b) = d$ if $d \mid a$, $d \mid b$, and if any other d' divides both a and b, $d' \mid d$.

Note that gcd of two numbers is not unique. If d satisfies the properties of gcd, then so does du for a unit u. However, if both d_1 and d_2 are greatest common divisors, then we must have $d_1 \mid d_2$ and $d_2 \mid d_1$. Therefore, gcd is unique up to a factor of some unit.

Proposition 2.3

Let R be a unique factorization domain. Then $\gcd(a,b)$ exists for all a, b.

We have deviated a lot from our original problem. Let's get back to it. Let d be a gcd of $y + \sqrt{2}i$ and $y - \sqrt{2}i$. Then d divides both of them, so d divides their difference $2\sqrt{2}i$. Since our norm function is multiplicative,

$$N(d) \mid N\left(2\sqrt{2}i\right) = 8\,.$$

Therefore, $N(d) \in \{1, 2, 4, 8\}$. If $N(d)$ is even, since $d \mid y + \sqrt{2}i$,

$$2 \mid N(d) \mid N\left(y + \sqrt{2}i\right) = y^2 + 2 \implies 2 \mid y\,.$$

But we are considering y odd. Therefore, $N(d) = 1$. So d must be 1 (or -1). So $y + \sqrt{2}i$ and $y - \sqrt{2}i$ have no common prime factor[2]. Now we want to argue that both $y + \sqrt{2}i$ and $y - \sqrt{2}i$ are perfect cubes.

Since $\mathbb{Z}\left[\sqrt{2}i\right]$ is a UFD, factorization into primes is unique (up to a factor of units). The only units of $\mathbb{Z}\left[\sqrt{2}i\right]$ are 1 and -1. Suppose p is a prime in $\mathbb{Z}\left[\sqrt{2}i\right]$ dividing x. Then p^3 divides either of $y + \sqrt{2}i$ and $y - \sqrt{2}i$. Now, since their prime factorization is unique, we can conclude that both of them are perfect cubes. In fact,

$$y + \sqrt{2}i = \left(a + b\sqrt{2}i\right)^3 \text{ and } y - \sqrt{2}i = \left(a - b\sqrt{2}i\right)^3$$

for some $a, b \in \mathbb{Z}$. Now, expanding these equations and solving for a and b, one finds that the only possibilities are $a = \pm 1$ and $b = 1$. From this, we can find that $y = \pm 5$. So $x = 3$. These are the only solutions.

Exercise 2.3

Find all pairs of integers (x, y) such that $x^2 = y^2 + 5$.

Let's try to do this the same way as above. After factorizing, we obtain

$$x^2 = \left(y + \sqrt{5}i\right)\left(y - \sqrt{5}i\right)\,.$$

In a similar spirit, we shall now work on the ring $\mathbb{Z}\left[\sqrt{5}i\right]$. One can show that $\gcd\left(y + \sqrt{5}i, y - \sqrt{5}i\right)$ is 1 when y is not divisible by 5. The case $5 \mid y$ is trivial, and can be solved by considering mod

[2] Technically speaking, we should say they don't have any common irreducible factors. But we are in a UFD. So prime and irreducible are the same thing here.

25. Therefore, by a similar argument as above, both $y+\sqrt{5}i$ and $y-\sqrt{5}i$ are perfect squares in $\mathbb{Z}\left[\sqrt{5}i\right]$.

$$y+\sqrt{5}i=\pm\left(a+b\sqrt{5}i\right)^2=\pm a^2\mp 5b^2\pm 2ab\sqrt{5}i\,.$$

Therefore, $1=\pm 2ab$, so there are no solutions!

But clearly that's not true at all. $(x,y)=(\pm 3,\pm 2)$ is clearly a solution to this equation. So where did we go wrong? Here we implicitly assumed that $\mathbb{Z}\left[\sqrt{5}i\right]$ is a UFD, and invoked unique factorization to argue that both $y+\sqrt{5}i$ and $y-\sqrt{5}i$ are perfect squares. But $\mathbb{Z}\left[\sqrt{5}i\right]$ is NOT a UFD. For instance, 9 does not have a unique factorization in $\mathbb{Z}\left[\sqrt{5}i\right]$.

$$9=3\cdot 3=\left(2+\sqrt{5}i\right)\left(2-\sqrt{5}i\right)\,,$$

and 3, $2+\sqrt{5}i$, $2-\sqrt{5}i$ are all irreducibles. So there does not exist a unique factorization into irreducibles. That's why this proof is wrong.

§3 Gaussian Integers

The reader is highly encouraged to show that the ring of Gaussian integers $\mathbb{Z}[i]$ is an ED, and hence a UFD. Gaussian integers are particularly useful in solving various number theory problems.

Exercise 3.1

Let p be a prime. Then $p=a^2+b^2$ if and only if $p\equiv 1 \pmod 4$.

Solution. For $p\equiv 3 \pmod 4$, p cannot be expressed as the sum of two squares, because the sum of two squares is either 0 or 1 or 2 in mod 4. Now let's consider the converse. Since $p\equiv 1 \pmod 4$, -1 is a quadratic residue. This can be seen by noting that

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=1\,.$$

So, there exists $n\in\mathbb{N}$ such that $p\mid n^2+1$. Now we shall work on $\mathbb{Z}[i]$.

$$p\mid n^2+1=(n+i)(n-i)\,.$$

Now suppose p is a prime in $\mathbb{Z}[i]$. Then p divides either of $n\pm i$. So, $n\pm i=p(a+bi)$ for some $a,b\in\mathbb{Z}$. Equating the imaginary parts, we get that $pb=\pm 1$. This is not possible since p is not a unit in $\mathbb{Z}$. Therefore, p is not a prime in $\mathbb{Z}[i]$. Hence,

$$p=(a+bi)(c+di)\,,$$

where neither $a+bi$ nor $c+di$ is a unit. The only units in $\mathbb{Z}[i]$ are $\pm 1,\pm i$. By taking norm on both sides, we find that

$$p^2=N(p)=N(a+bi)\,N(c+di)=\left(a^2+b^2\right)\left(c^2+d^2\right)\,.$$

a^2+b^2 cannot be 1, because then $a+ib$ becomes a unit. For the same reason c^2+d^2 cannot be 1. Therefore, we must have $p=a^2+b^2=c^2+d^2$. ■

We have seen that every prime of the form $4k+1$ can be expressed as the sum of two squares. But is this expression unique? Can there be multiple ways of expressing a prime as a sum of two integers?

Exercise 3.2
If $p = a^2 + b^2$, a and b are unique up to order and sign.

Solution. Suppose $p = a^2 + b^2 = c^2 + d^2$. Factorizing in $\mathbb{Z}[i]$, we get

$$(a + bi)(a - bi) = (c + di)(c - di) .$$

$N(c \pm di) = N(a \pm bi) = p$ is a prime in $\mathbb{N}$, so $a \pm bi$ and $c \pm di$ are all primes in $\mathbb{Z}[i]$. Because otherwise,

$$\alpha\beta = a \pm bi \implies N(\alpha) N(\beta) = N(a \pm bi) = p \implies N(\alpha) = 1 \text{ or } N(\beta) = 1 ,$$

which means α or β is a unit. Since $\mathbb{Z}[i]$ is a UFD,

$$a + bi = u(c + di) \quad \text{or} \quad a + bi = u(c - di) ,$$

for some unit $u \in \mathbb{Z}[i]$. Now, $u \in \{1, -1, i, -i\}$, so considering these cases one can show that $\{a^2, b^2\} = \{c^2, d^2\}$. ■

Exercise 3.3 (Pythagorian triples)
Find all triples of integers (x, y, z) such that $x^2 + y^2 = z^2$ and $\gcd(x, y) = 1$.

It is possible to show using elementary methods that the general form of Pythagorian triples is $(x, y, z) = \left(m^2 - n^2, 2mn, m^2 + n^2\right)$, where $m - n$ is odd. Here we shall see a solution involving Gaussian integers.

Solution. Note that, x and y must have different parity. If they both are even, $\gcd(x, y) = 1$ is not satisfied. If both of them are odd, z is even. But then, taking mod 4 yields a contradiction. Therefore, we can assume WLOG that x is odd and y is even. Then z is odd. Factorizing in $\mathbb{Z}[i]$, we get

$$z^2 = x^2 + y^2 = (x + iy)(x - iy) .$$

Now we claim that $\gcd(x + iy, x - iy) = 1$ in $\mathbb{Z}[i]$. Let d be a Gaussian integer that divides both $x + iy$ and $x - iy$. Then we get $d \mid 2x$ and $d \mid 2yi$. $d \mid 2$ contradicts with z being odd. Therefore, $d \mid x$ and $d \mid y$. Taking norms, we get

$$N(d) \mid x^2 \text{ and } N(d) \mid y^2 .$$

Since $\gcd(x, y)$ in $\mathbb{Z}$, $N(d)$ must be 1, which indicates that d is a unit. Hence, $\gcd(x + iy, x - iy) = 1$.

Now, since $\mathbb{Z}[i]$ is a UFD, both $x + iy$ and $x - iy$ are perfect squares (up to a factor of some unit) in $\mathbb{Z}[i]$. Therefore,

$$x + iy = u(a + ib)^2 = u\left(a^2 - b^2 + 2xyi\right) ,$$

for some unit u. Since we assumed y is even, u is either 1 or -1. Therefore, we find that

$$(x, y, z) = \left(a^2 - b^2, 2ab, a^2 + b^2\right) ,$$

for $a, b, c \in \mathbb{Z}$ with a and b having different parity. Because otherwise, $\gcd(x, y) = 1$ condition is violated. ■

Like $\mathbb{Z}$, $\mathbb{Z}[i]$ also has primes. What do these primes look like? One can easily check that not every primes in $\mathbb{Z}$ stays prime in $\mathbb{Z}[i]$. For instance, 5 is not a prime in $\mathbb{Z}[i]$, because

$$5 = (1+2i)(1-2i) .$$

But what about these factors $1+2i$ and $1-2i$? Are they primes? One can show that they are, indeed, primes in $\mathbb{Z}[i]$. Because if α divides $1+2i$, by taking norm, we get

$$N(\alpha) \mid N(1+2i) = 5 .$$

This indicates that $1+2i$ does not have any nontrivial factors. This way one can show that the prime numbers of $\mathbb{Z}$ of the form $4k+1$ are not primes in $\mathbb{Z}[i]$, but their factors are.

Now what about primes of the form $4k+3$? They cannot be expressed as sum of two squares. So they aren't reducible in $\mathbb{Z}[i]$, right? The details are left as an exercise for the reader to fill in.

Theorem 3.1

Every prime in $\mathbb{Z}[i]$ is a unit multiple of one of the following:

(i) $1+i$

(ii) p, where $p \equiv 3 \pmod 4$ is a prime in $\mathbb{Z}$

(iii) $a+bi$, where $a^2+b^2 = p$ for some prime $p \in \mathbb{Z}$

Exercise 3.4

An integer greater than 1 is a sum of two squares if and only if any prime factor p with $p \equiv 3 \pmod 4$ occurs with even multiplicity.

Solution. The if direction is easy, so we leave it as an exercise for the reader. We shall do the only if direction. Suppose $n \geq 2$ is an integer such that $n = a^2+b^2$. We shall proceed by strong induction on n. The base case $n = 2$ is true, because it has no prime factor of the form $4k+3$. Now assume $n \geq 3$, and the statement is true for every m smaller than n.

If n has no prime factors of the form $4k+3$, then the statement is vacously true. Suppose $p \mid n = a^2+b^2$ where $p \equiv 3 \pmod 4$.

$$p \mid n = a^2+b^2 = (a+ib)(a-ib) .$$

p is a prime in $\mathbb{Z}[i]$ by Theorem 3.1. Therefore, p divides either of $a \pm ib$. As a result, $a \pm ib = p(c \pm id)$, so p divides both a and b. Hence, $a = pa'$ and $b = pb'$ for some integers a, b.

$$n = a^2+b^2 = p^2\left(a'^2+b'^2\right) .$$

$a'^2+b'^2$ is a sum of two sqaures and it is smaller than n. Therefore, by inductive hypothesis, every prime of the form $4k+3$ has even multiplicity in $a'^2+b'^2$. Since n and $a'^2+b'^2$ differs only by a factor of p^2, we can conclude that the statement is true for n as well. ∎

§4 Polynomials

We have seen earlier that the set of all polynomials with coefficients in a ring R forms a ring, and we denote this ring by $R[x]$. If R is an integral domain, then so is $R[x]$.

Proposition 4.1

If F is a field, $F[x]$ is an Euclidean Domain.

Proof. The Euclidean function in $F[x]$ is $N(f) = \deg f$. □

Now we shall see some interesting properties of polynomial rings, for which we need some more definitions.

Definition 4.1 (Ideal)**.** A subset $I \subseteq R$ is an **ideal**, written $I \trianglelefteq R$, if

(i) It is an additive subgroup of R, i.e. it is closed under addition and additive inverses.

(ii) If $x \in I$ and $r \in R$, then $rx \in I$.

An ideal I is called **principal** if it is generated by a single element. That is, there exists $a \in R$ such that

$$I = \{ra \mid r \in R\} .$$

We write it as $I = (a)$.

Definition 4.2 (Principal Ideal Domain)**.** An integral domain R is a **Principal Ideal Domain** (PID) if every ideal is a principal ideal.

Proposition 4.2

R is an ED $\implies$ R is a PID $\implies$ R is a UFD.

Proposition 4.3

$F[x]$ is a PID if and only if F is a field.

Theorem 4.4 (Bézout's Identity)

Let R be a PID, and $a, b \in R$ with $\gcd(a, b) = d$. Then there exist $x, y \in R$ such that $ax + by = d$.

In general, Bézout's identity does not hold when R is not a PID. In particular, if R is not a field, Bézout's identity is not true in $R[x]$. For instance, let $2x, x^2 \in \mathbb{Z}[x]$. Their gcd is x. But there do not exist integer polynomials $f, g \in \mathbb{Z}[x]$ such that

$$2xf + x^2 g = x .$$

Exercise 4.1 (USA TST 2016)

Define $\Psi : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ by

$$\Psi\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_i x^{p^i} .$$

Prove that for nonzero polynomials $F, G \in \mathbb{F}_p[x]$, $\Psi(\gcd(F, G)) = \gcd(\Psi(F), \Psi(G))$.

In case you're not familiar with the notation, $\mathbb{F}_p$ denotes the field of integers modulo p, where p is a prime number.

Solution Outline. First, show that Ψ is additive. Furthermore, if $P \mid Q$, then $\Psi(P) \mid \Psi(Q)$ for $P, Q \in \mathbb{F}_p[x]$. Let $D = \gcd(F, G)$, and $D' = \gcd(\Psi(F), \Psi(G))$. We need to show that $\Psi(D) = D'$.

D divides both F and G, so $\Psi(D)$ divides both $\Psi(F)$ and $\Psi(G)$. Therefore,

$$\Psi(D) \mid \gcd(\Psi(F), \Psi(G)) = D'.$$

Since $\mathbb{F}_p$ is a field, $\mathbb{F}_p[x]$ is a PID. Therefore, Bézout's identity holds here. So, there exists $A, B \in \mathbb{F}_p[x]$ such that

$$AF + BG = \gcd(F, G) = D \implies \Psi(AF) + \Psi(BG) = \Psi(D).$$

Now, $D' \mid \Psi(F) \mid \Psi(AF)$. Similarly, $D' \mid \Psi(BG)$. Therefore, $D' \mid \Psi(D)$. Hence, $D' = \Psi(D)$. ■

Exercise 4.2 (IMC 2020)
Find all prime numbers p such that there exists a unique $a \in \mathbb{F}_p$ for which $a^3 - 3a + 1 = 0$.

Solution. We need to find all p such that the polynomial $x^3 - 3x + 1 \in \mathbb{F}_p[x]$ has a unique root a. In other words, either $x^3 - 3x + 1 = (x - a)^3$ or $x^3 - 3x + 1 = (x - a) P(x)$ for some irreducible quadratic polynomial $P \in \mathbb{F}_p[x]$. For the first case, $3a = 0$ with $a \neq 0$, so $p = 3$. Let's consider the latter case now.

$$x^3 - 3x + 1 = (x - a)\left(x^2 + \alpha x + \beta\right) \implies \alpha = a, \beta = -a^{-1}.$$

The quadratic $x^2 + ax - a^{-1}$ is irreducible. Hence, its discriminant Δ is not a square of any number in $\mathbb{F}_p$. In other words, $\Delta = a^2 + 4a^{-1}$ is not a quadratic residue modulo p.

$$a^3 - 3a + 1 = 0 \implies a\left(a^2 - 3\right) = -1 \implies a^2 = 3 - a^{-1} \implies \Delta = 3\left(1 + a^{-1}\right).$$

Now, let $b = 1 + a^{-1}$. Substituting this into our original equation $a^3 - 3a + 1 = 0$, we get

$$(b-1)^3 - 3(b-1)^2 + 1 = 0 \implies b(b-3)^2 = 3 \implies \Delta 3b = b^2(b-3)^2.$$

So Δ is a quadratic residue modulo p, and hence $x^2 + ax - a^{-1}$ is reducible. Therefore, no such p in this case. ■

§5 A "Proof" of Fermat's Last Theorem

Theorem 5.1 (Fermat's Last Theorem)
The equation

$$x^n + y^n = z^n$$

has no solution in positive integers if $n \geq 3$.

We shall first consider the case $n = 3$ and then we will generalize. Firstly, we can assume WLOG that x, y, z have no common factors. Also, one can show that $3 \nmid y$ and $3 \nmid z$. Let ω be the primitive cubic root of unity, i.e. $\omega = e^{\frac{2\pi i}{3}}$. Then we have

$$x^3 - 1 = (x-1)(x-\omega)\left(x-\omega^2\right) \implies x^3 + 1 = (x+1)(x+\omega)\left(x+\omega^2\right).$$

Using this, we can factorize $x^3 + y^3$.

$$z^3 = x^3 + y^3 = (x+y)(x+y\omega)\left(x+y\omega^2\right).$$

Now we want to show that these three factors are pairwise co-prime, i.e. pairwise gcd 1. Suppose p is a prime in $\mathbb{Z}[\omega]$ such that $p \mid x + y$ and $p \mid x + y\omega$. Then p must divide $(\omega - 1)y$ and $(\omega - 1)x$. Since x and y do not have any common divisor, p must divide $\omega - 1$. But $\omega - 1$ divides 3, because

$$(\omega-1)^2 + 3(\omega-1) = -3 \implies (\omega-1)(\omega+2) = -3.$$

So p divides 3. But z is coprime with 3, so p must be 1. Hence, $\gcd(x+y, x+y\omega) = 1$. In a similar manner, one can show that the other factors are also pairwise coprime.

Now, the product of some pairwise coprime numbers is a perfect cube, so the factors must also be a perfect cube.

$$x + y\omega = ua^3 \quad \text{and} \quad x + y\omega^2 = \bar{u}\bar{a}^3.$$

for some unit u. Firstly, consider $u = 1$. Let $a = m + n\omega$, so $\bar{a} = m + n\omega^2$. After expanding and subtracting one from the other, we get

$$y\left(\omega - \omega^2\right) = 3\left(m^2 n - mn^2\right)\left(\omega - \omega^2\right) \implies y = 3\left(m^2 n - mn^2\right).$$

But $3 \nmid y$, so this yields a contradiction. Similarly, for $u = \omega$ and $u = \omega^2$, one obtains an analogous contradiction. Therefore, $x^3 + y^3 = z^3$ has no solutions in $\mathbb{Z}^+$.

Gabriel Lamé showed that it suffices to consider the case when n is a prime number. He generalized this very idea we used in order to solve the case $n = 3$. Suppose $n = p$ is a prime number, and let ω be the primitive p-th root of unity, i.e. $\omega = e^{\frac{2\pi i}{p}}$. Using this, we can factorize $x^p + y^p$.

$$z^p = x^p + y^p = (x+y)(x+y\omega)\left(x+y\omega^2\right)\cdots\left(x+y\omega^{p-1}\right).$$

As before, you can show that $p \nmid y$ and $p \nmid z$. Also, these factors are relatively coprime which can be shown in a similar manner as above. Therefore, these factors are all perfect p-th power. Therefore,

$$x + y\omega = ua^p \quad \text{and} \quad x + y\omega^{p-1} = \bar{u}\bar{a}^p,$$

for some unit u. Suppose $u = 1$. Subtracting one from the other, we get

$$y\left(\omega - \omega^{p-1}\right) = a^p - \bar{a}^p.$$

The RHS is divisible by p. This can be shown by expanding. However, p is coprime with $\omega - \omega^{p-1}$. Therefore, $p \mid y$. But this is a contradiction. Similarly, considering $u = \omega^i$, one obtains an analogous contradiction. So $x^p + y^p = z^p$ has no solutions in $\mathbb{Z}^+$.

Other than the omitted details, this proof seems fine, right? But actually it's not. There is a hidden assumption that $\mathbb{Z}[\omega]$ is a UFD. But that's not true for every p. In fact, it holds only for finitely many p. While these algebraic tools are really useful in order to solve various number theory problems, we need to be extremely careful about each of our claims and reasonings behind steps.

§6 Practice Problems

Problem 6.1. Show that $\mathbb{Z}\left[\sqrt{2}i\right]$ is an ED with the norm function $N\left(x+y\sqrt{2}i\right)=x^2+2y^2$.

Problem 6.2. Show that $\gcd\left(y+\sqrt{5}i, y-\sqrt{5}i\right)=1$ for $5\nmid y$.

Problem 6.3. Show that $\mathbb{Z}[i]$ is an ED with the norm function $N(x+yi)=x^2+y^2$.

Problem 6.4. Find all pairs of integers (x,y) such that $x^3=y^2+4$.

Problem 6.5. Find all triples of integers (x,y,z) such that $x^2+y^2=z^n$ and $\gcd(x,y)=1$.

Problem 6.6. Find all pairs of integers (x,y) such that $x^2+1=y^n$ for some integer $n>1$.

Problem 6.7. Prove Theorem 3.1.

Problem 6.8. Fill in the details of Exercise 4.1.

Problem 6.9. Prove that $\mathbb{Z}[\omega]$ is an ED, where ω is the primitive cubic root of unity.

Problem 6.10. Find all pair of integers (x,y) such that

$$x^2-x+1=y^3\,.$$

Problem 6.11. Find all pair of integers (x,y) such that

$$x^2+x+2=y^3\,.$$

Problem 6.12. If x,y,z are positive integers satisfying $x^3+y^3=z^3$, show that $3\nmid y$ and $3\nmid z$.

Problem 6.13. Solve the $n=3$ case of Fermat's last theorem by working on $\mathbb{Z}\left[\sqrt{3}i\right]$.

Problem 6.14. Find all pairs (x,y) of positive integers such that

$$13^x+3=y^2\,.$$

Problem 6.15. Solve the equation

$$x^2+3=y^n\,,$$

where n is an integer greater than 1.

Problem 6.16. Solve the equation

$$x^2+9=y^n\,,$$

where n is an integer greater than 1.

Problem 6.17. Solve the equation

$$x^2+11=3^n\,,$$

where n is an integer greater than 1.

Problem 6.18. Let a and b be positive integers such that $b=x^2-dy^2$ for some integers x,y,d with $d=a^2-1$. Prove that if $b<2(a+1)$, then b is a perfect square.